Our Reference: GP-303855-OST-ALS PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	William L. Ball
Serial Number:	10/712,480
Filing Date:	November 13, 2003
Confirmation No.:	8336
Examiner/Group Art Unit:	Natalie Pass/3686
Title:	SYSTEM AND METHOD FOR MAINTAINING AND PROVIDING PERSONAL INFORMATION IN REAL TIME

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Please enter the following Appeal Brief in the appeal filed May 18, 2010. Since July 18, 2010 fell on a weekend, it is submitted that this Appeal Brief is being timely filed.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real parties in interest are Assignee 1) General Motors LLC, by assignment from General Motors Corporation, and 2) OnStar LLC, having common ownership with General Motors LLC. General Motors LLC is a corporation having an office and a place of business at 300 Renaissance Center, Detroit, Michigan 48265-3000. The Appellant also notes that security interests have been recorded.

II. RELATED APPEALS AND INTERFERENCES

Appellant and the undersigned attorney are not aware of any appeals or any interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-3, 7, 9-11, 13, and 16-23 are the claims on appeal. *See,* Appendix.

Claims 4-6, 8, 12, 14, and 15 were canceled.

Claims 1-3, 7, 9-11, 13, and 16-23 were rejected.

IV. STATUS OF AMENDMENTS

In response to the Final Office Action of February 18, 2010, no amendment pursuant to 37 C.F.R. § 1.116 was filed.

V. SUMMARY OF CLAIMED SUBJECT MATTER

In this summary of claimed subject matter, all citations are to the specification of United States Patent Application 10/712,480. Further, all citations are illustrative, and support for the cited element may be found elsewhere in the specification.

Independent claim 1:

Independent claim 1 is directed to a system for providing medical information of a vehicle user. As shown in Figs. 1 and 2 of Appellant's application as filed, the system 100 comprises: a key device 120 corresponding to a particular vehicle 110, the key device 120 having stored therein an encryption code associated with the medical information of the vehicle user (see page 4, line 24 through page 5, line 5; page 16, lines 2-15; and Figs. 1 and 2 of Appellant's application as filed); a transient memory storage 118 located within the particular vehicle 110 and in communication with the key device 120 (see page 5, lines 6-13 and Figs. 1 and 2 of Appellant's application as filed), the transient memory storage 118 configured to i) receive a transmission of the encryption code from the key device 120 prior to an emergency event (see page 16, lines 16-28 of Appellant's application as filed), and ii) temporarily store the encryption code prior to the emergency event (see page 17, lines 2-9 of Appellant's application as filed); a telematics unit 130 in communication with the transient memory storage 118 device and configured to receive a transmission of the encryption code from the transient memory storage 118 in response to the emergency event involving the particular vehicle 110 (see page 5, lines 9-13; pages 17-18; and Figs. 1 and 2 of Appellant's application as filed); and a call center 180 in wireless communication with the telematics unit 130 via a wireless network (see Fig. 1 and page 8 of Appellant's application as filed), wherein the call center 180 is configured to i) receive a transmission of the encryption code from the telematics unit 130 in response to the emergency event (see page 17, lines 10-19 of Appellant's application as filed), and ii) transfer the received encryption code to emergency personnel (see page 17, lines 20-24 of Appellant's application as filed).

Independent claim 11:

Independent claim 11 is directed to a method for providing medical information of a vehicle user. The method comprises: storing an encryption code in a key device 120 corresponding to a particular vehicle 110, the encryption code associated with the medical information stored in a database (see page 4, line 24 through page 5, line 5; page 16, lines 2-15; and Figs. 1 and 2 of Appellant's application as filed); transmitting the encryption code from the key device 120 to a vehicle storage unit (such as, e.g., the transient storage 118) of the particular vehicle 110 and temporarily storing the transmitted encryption code in the vehicle storage unit 118 prior to an emergency event (see page 5, lines 6-13; page 16, lines 16-28; page 17, lines 2-9; and Figs. 1 and 2 of Appellant's application as filed); transmitting, from the vehicle storage unit 118 to an in-vehicle telematics unit 130 of the particular vehicle 110 and from the in-vehicle telematics unit 130 to a call center 180, the temporarily stored encryption code in response to the emergency event involving the particular vehicle (see page 5, lines 9-13; pages 17-18; and Figs. 1 and 2 of Appellant's application as filed); transmitting the encryption code from the call center 180 to an emergency personnel (see page 17, lines 20-24 of Appellants' application as filed); and accessing, via the emergency personnel, the medical information from the database using the encryption code (see page 18, lines 15-19 of Appellant's application as filed).

Independent claim 17:

Independent claim 17 is directed to a system for providing medical information of a vehicle user. The system 100 comprises: key device means (such as, e.g., the key device 120) corresponding to a particular vehicle 110 for receiving and storing an encryption code, the encryption code associated with the medical information of the vehicle user stored in a database (see page 4, line 24 through page 5, line 5; page 16, lines 2-15; and Figs. 1 and 2 of Appellant's application as filed); vehicle storage means (such as, e.g., the transient memory 118) of the particular vehicle 110 for i) receiving a transmission of the encryption code from the key device means prior to an emergency event, and ii) temporarily storing the encryption code prior to the emergency event (see page 5, lines 6-13; page 16, lines 16-28; page 17, lines 2-9; and Figs. 1 and 2 of Appellant's application as filed); an in-vehicle telematics unit 130 of the particular vehicle

110 in communication with the vehicle storage means (see page 5, lines 9-13 and Fig. 1 of Appellant's application as filed); means for transmitting i) from the vehicle storage means 118 to the in-vehicle telematics unit 130, and ii) from the in-vehicle telematics unit 130 to a call center 180, the temporarily stored encryption code in response to the emergency event involving the particular vehicle 110 (see page 5, lines 9-13; page 17, lines 10-19; and Fig. 1 of Appellant's application as filed); and means for accessing, via the emergency personnel, the medical information from the database using the encryption code (see page 18, lines 15-19 of Appellant's application as filed).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant requests review of the following grounds of rejection on appeal:

1) Whether claims 1-3, 9, 11, 13, 17, 20, and 22 are unpatentable under 35 U.S.C. § 103(a) over U.S. Patent Publication No. 2001/0034223 to Rieser, et al. (referred to herein as "Rieser") in view of U.S. Patent No. 5,949,152 to Tagawa, et al. (referred to herein as "Tagawa"), and further in view of U.S. Patent Publication No. 2002/0003571 to Schofield, et al. (referred to herein as "Schofield").

2) Whether claims 16 and 19 are unpatentable under 35 U.S.C. § 103(a) over Rieser, Tagawa, and Schofield, and further in view of U.S. Patent Publication No. 2003/0109245 to McCalmont, et al. (referred to herein as "McCalmont").

3) Whether claims 7, 10, 18, 21, and 23 are unpatentable under 35 U.S.C. § 103(a) over Rieser, Tagawa, and Schofield, and further in view of U.S. Patent No. 6,526,335 to Treyz, et al. (referred to herein as "Treyz").

VII. ARGUMENTS

The arguments presented hereinbelow address the rejection(s) stated in the Final Office Action dated February 18, 2010. It is submitted, however, that the absence of a reply to a specific rejection, issue or comment in the Final Office Action does not signify agreement with or concession of that rejection, issue or comment. Finally, nothing in the following arguments of this appeal brief should be construed as an intent to concede any issue with regard to any claim, except if specifically stated below.

A. Rejection of claims 1-3, 9, 11, 13, 17, 20, and 22 under 35 U.S.C. § 103(a) over Rieser, Tagawa, and Schofield

In the Final Office Action dated February 18, 2010, claims 1, 11, and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Rieser, Tagawa, and Schofield. The Examiner asserted that the combination of Rieser and Tagawa discloses all of the elements of claim 1, 11, and 17, except for i) storing an encryption code in a key device corresponding to a particular vehicle, and ii) transmitting, from the vehicle storage unit to an in-vehicle telematics unit of the particular vehicle and from the in-vehicle telematics unit to a call center, the temporarily stored encryption code in response to the emergency event involving the particular vehicle. The Examiner's reasoning for her assertion stated above is set forth in the Office Action dated August 14, 2009. The Examiner further asserted that the foregoing deficiencies of Rieser and Tagawa are well known in the art, as evidenced by Schofield. The Examiner concluded that the combination of Rieser, Tagawa, and Schofield renders obvious independent claims 1, 11, and 17.

At the outset, obviousness is a question of law based on i) the scope and content of the prior art, ii) the differences between the prior art and the claims at issue, iii) the level of ordinary skill in the art, and iv) objective evidence of non-obviousness (*Graham v. John Deere Co.,* 383 U.S. 1, 17, 148 USPQ 459, 467 (1966)). An invention may be obvious if it merely combines "familiar elements according to known methods [to] yield predictable results" (*KSR Int. Co. v. Teleflex Inc, et al.*, 127 S. Ct. 1727; 167 L.Ed.2d 705; 2007 U.S. LEXIS 4745; 75 U.S.L.W. 4289; 82 USPQ2d 1385 (2007)).

A basic requirement to establish a *prima facie* case of obviousness is that "the prior art reference (or references when combined) must teach or suggest all the claim limitations" (emphasis added; see MPEP § 2143). "In proceeding before the Patent and Trademark Office, the Examiner bears the burden of establishing a *prima facie* case of obviousness based upon the prior art" (*In re Fritch*, 972 F.2d 1260, 1265, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992)). "If examination at the initial stage does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to grant of the patent" (*In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)).

In light of the precedent cited above, Appellant submits that the Examiner has *failed* to establish a *prima facie* case of obviousness over claims 1, 11, and 17, at least because the combination of Rieser, Tagawa, and Schofield *fails* to disclose or suggest all of the elements of claims 1, 11, and 17.

Independent claims 1 and 17 are both directed to a system for providing medical information of a vehicle user, and independent claim 11 is directed to a method for accomplishing the same. The system defined in claims 1 and 17 includes, in part and in some form, a transient memory storage located within the vehicle and in communication with the key device, where the transient memory storage is configured to i) receive a transmission of the encryption code from the key device prior to an emergency event, and ii) temporarily store the encryption code prior to the emergency event. The method defined in claim 11 includes, in part, transmitting the encryption code from the key device to a vehicle storage unit and temporarily storing the transmitted encryption code in the vehicle storage unit prior to the emergency event.

Rieser discloses a method and system for providing location dependent and personal identification information to a public safety answering point. The method and system uses a small hand-held device (a personal security transmitter 105) that may be quickly and easily activated by an individual in need of help and provides public safety personnel (e.g., police) with at least the individual's location and personal identification information (see, e.g., paragraph [0007] of Rieser). In an example, the personal security transmitter sends a transmission signal packet ***upon activation***, which is received by a base station (e.g., mounted in a police vehicle). (See paragraphs [0029] and [0075] of Rieser.) Upon receiving the transmission signal packet,

the base station generates a base station packet and transmits the base station packet to a command center. The command center processes the packet information to alert personnel that a *call for assistance has been received*. (See paragraph [0029] of Rieser.) Appellant submits that Rieser does *not* disclose or suggest that the transmission signal packet is temporarily stored in a storage unit located within the base station (as similarly recited in claims 1, 11, and 17).

Appellant further submits that the Rieser disclosure is directed to a security communications system for a college campus (see paragraph [0003]). As is evident by the portions of Rieser cited above, it is submitted that the security communication system is an on-demand system. For instance, a call for assistance is made by activating the personal security transmitter. To reiterate from above, upon activating the personal security transmitter, a transmitter identification number (which may be used to identify the transmitter sending the transmission) is sent to the base station, which processes the transmission and sends it to a command center. In other words, the transmitter identification number is sent to the base station ***at the time*** the emergency event occurs. This is in sharp contrast to Appellant's system (as defined in claims 1 and 17) and method (as defined in claim 11), whereby the encryption code is transmitted to and temporarily stored in the storage unit in the vehicle ***prior to*** an emergency event. As such, when an emergency event occurs, the encryption code may be retrieved from the storage unit and transmitted to a call center (via, e.g., an in-vehicle telematics unit).

Additionally, claim 11 recites, in part, i) transmitting an encryption code from a key device to a vehicle storage unit and temporarily storing the encryption code prior to an emergency event, and ii) in response to an emergency event, transmitting the encryption code from the vehicle storage unit ***to an in-vehicle telematics unit*** and then to a call center. Claim 11 further recites that the key device corresponds to a particular vehicle, the telematics unit corresponds to the particular vehicle, and the emergency event involves the particular vehicle.

Referring again to Rieser, the reference also discloses that the base station may be a mobile base station (such as, e.g., a campus police vehicle). When an emergency event occurs, the identification number of the transmitter may be transmitted to the mobile base station, and identification information (e.g., medical history) may be retrieved from a database at the mobile base station (see paragraphs [0032], [0033], and [0075] of Rieser). Thus, when an emergency

event occurs, the identification number is transmitted from the user of the transmitter to the mobile base station (e.g., the campus police vehicle). Appellant points out that the mobile base station in Rieser is ***not*** the vehicle actually involved in the emergency event. Thus, the identification number is ***not*** transmitted from the key device ultimately to ***the vehicle actually involved in the emergency event***.

Yet further, claims 1, 11, and 17 recite that the encryption code is transmitted from a transient memory storage to a ***telematics unit*** of the vehicle. In sharp contrast, Rieser discloses that "[a] wireless communications link can be used to connect a mobile base station to a remote command center…" (paragraph [0075]). Appellant submits that Rieser neither discloses nor suggests that the wireless communication link involves a telematics unit or other vehicle-dedicated communications technology.

Appellant submits that the Tagawa reference *fails* to supply at least some of the deficiencies of Rieser identified above. Tagawa discloses an antitheft system for a vehicle having an immobilizer unit that reads an identification code transmitted by an ignition key (see abstract and column 4, lines 50-58 of Tagawa). The identification code is transmitted when the ignition key turns on the ignition switch of the vehicle (column 4, lines 59-63). Appellant submits that Tagawa does *not* disclose transmitting the identification code when the vehicle is involved in an emergency event.

Tagawa further discloses that the identification code is transmitted from the ignition key to the immobilizer unit and, if the identification code on the ignition key does not correspond with the registered identification code, the immobilizer unit automatically changes the function mode of an engine controlling unit to prohibit starting up the engine (see column 4, lines 50-58). It is submitted that Tagawa does *not* disclose or suggest transmitting the identification code to a telematics unit or to another vehicle dedicated communications device.

As mentioned above, in the Final Office Action dated February 18, 2010, the Examiner admitted that Rieser and Tagawa fail to disclose i) storing ***an encryption code*** in a key device corresponding to a particular vehicle, and ii) transmitting ***the encryption code*** in response to an emergency event involving the particular vehicle. The Examiner asserted, however, that the

foregoing elements are well known in the art, as evidenced by the Schofield reference. Appellant respectfully disagrees with the Examiner's assertion for the reasons stated below.

Schofield discloses a rear view mirror for a vehicle including a video display assembly (see abstract of Schofield). The rear view mirror assembly may include accessories, such as a phone (see, e.g., paragraph [0256]) that may be traceable via a GPS system (see, e.g., paragraph [0257]). Schofield further notes that cellular phones will also become traceable via the GPS system (which may identify the cellular phone via a unique identifier), and therefore an emergency phone call made from a GPS to a, e.g., "911" service may be routes to a correct emergency agency (paragraph [0315]). In the Final Office Action, the Examiner argued that the "unique identifier" of the cellular phone that the GPS system may use to identify the phone is the same as an encryption code. Appellant disagrees with the Examiner, and submits that one skilled in the art would be cognizant of the fact that the unique identifier is a *mobile dialing number (MDN)* of the cellular phone; and not an encryption of medical information of, e.g., the owner of the cellular phone.

Schofield further discloses that tracing of the phone may be incorporated into or used in conjunction with a vehicle navigation system (paragraph [0315]). The Examiner asserted that such disclosure establishes that the phone is the same as a *key device* for a particular vehicle. At the outset, Appellant submits that a cellular phone is generally designated for a particular *user*; not for a particular vehicle. This is in sharp contrast to a "key device", which is a device that is linked to the vehicle. As disclosed by Appellant, the key device (which may be in the form of a key fob) controls basic services such as unlocking doors, defining programmable steering wheel buttons, seat positions, radio stations, etc. (see, e.g., page 10, lines 2-8 of Appellant's application as filed). As further disclosed by Appellant, the vehicle may have several key devices; one for each driver (page 11, lines 2-3of Appellant's application as filed). As such, it is submitted that the cellular phone disclosed in Schofield is *not* the same as the key device recited in Appellant's pending claims.

Additionally, Schofield discloses that the in-vehicle security system transmits images (taken, e.g., from a camera associated with the rear view mirror assembly) and/or vehicle data by wireless communication to a receiver remote from the vehicle (paragraph [0316]). Appellant

submits that i) Schofield does *not* disclose that the images and/or vehicle data are encrypted, and ii) Schofield does *not* disclose that the images and/or vehicle data are associated with medical information. Appellant further submits that the so-called "encryption code" associated with the cellular phone (more particularly, the identification number) is *not* transmitted to a remote facility (such as a call center) in response to an emergency event. As one skilled in the art would know, the identification number (or mobile dialing number) of the cellular phone is not transmitted; rather such number is used to establish a connection with the phone.

For all of the reasons stated above, Appellant submits that the combination of Rieser, Tagawa, and Schofield does *not* disclose all of the elements of independent claims 1, 11, and 17, and those claims depending therefrom. As such, it is submitted that the Examiner has *failed* to establish a *prima facie* case of obviousness under 35 U.S.C. § 103(a).

B. Rejection of claims 16 and 19 under 35 U.S.C. § 103(a) over Rieser, Tagawa, Schofield, and McCalmont

Appellant herein reiterates all of the arguments presented above in conjunction with the rejection of independent claim 11 (from which claim 16 depends) and independent claim 1 (from which claim 19 depends). For these reasons, it is submitted that independent claims 1 and 11 are patentable, and that claims 19 and 16 are also patentable at least because of their dependency from claims 1 and 11, respectively. As such, it is submitted that Appellant's invention as defined in claims 16 and 19 is not anticipated, taught, or rendered obvious by Rieser, Tagawa, Schofield, and McCalmont, either alone or in combination, and patentably defines over the art of record.

B. Rejection of claims 7, 10, 18, 21, and 23 under 35 U.S.C. § 103(a) over Rieser, Tagawa, Schofield, and Treyz

Appellant herein reiterates all of the arguments presented above in conjunction with the rejection of independent claim 1 (from which claims 7 and 10 depend), independent claim 11 (from which claims 21 and 23 depend), and independent claim 17 (from which claim 18 depends). For these reasons, it is submitted that independent claims 1, 11, and 17 are patentable,

and that claims 7, 10, 18, 21, and 23 are also patentable at least because of their dependency from one of claims 1, 11, and 17. As such, it is submitted that Appellant's invention as defined in claims 7, 10, 18, 21, and 23 is not anticipated, taught, or rendered obvious by Rieser, Tagawa, Schofield, and Treyz, either alone or in combination, and patentably defines over the art of record.

SUMMARY

The Appellant respectfully submits that claims 1-3, 7, 9-11, 13, and 16-23 as currently pending fully satisfy the requirements of 35 U.S.C. §§ 102, 103 and 112. Accordingly, Appellant respectfully requests that the Board of Patent Appeals and Interferences find for the Appellant and reverse the rejection of Appellant's claims 1-3, 9, 11, 13, 17, 20, and 22 under 35 U.S.C. § 103(a) as being unpatentable over Rieser, Tagawa, and Schofield; claims 2, 3, 9, 13, 20, and 22 under 35 U.S.C. § 103(a) as being unpatentable over Rieser, Tagawa, Schofield, and McCalmont; and claims 7, 10, 18, 21, and 23 under 35 U.S.C. § 103(a) as being unpatentable over Rieser, Tagawa, Schofield, and Treyz. In view of the foregoing, favorable consideration and passage to issue of the present application is respectfully requested. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

DIERKER & ASSOCIATES, P.C.

/Julia Church Dierker/

Julia Church Dierker
Attorney for Appellant
Registration No. 33368
(248) 649-9900, ext. 25
juliad@troypatent.com

3331 West Big Beaver Rd., Suite 109
Troy, Michigan 48084-2813

Dated: July 19, 2010

JCD/AMS

VIII. CLAIMS APPENDIX

1. (Previously presented) A system for providing medical information of a vehicle user, comprising:

a key device corresponding to a particular vehicle, the key device having stored therein an encryption code associated with the medical information of the vehicle user;

a transient memory storage located within the particular vehicle and in communication with the key device, the transient memory storage configured to i) receive a transmission of the encryption code from the key device prior to an emergency event, and ii) temporarily store the encryption code prior to the emergency event;

a telematics unit in communication with the transient memory storage device and configured to receive a transmission of the encryption code from the transient memory storage in response to the emergency event involving the particular vehicle; and

a call center in wireless communication with the telematics unit via a wireless network, wherein the call center is configured to i) receive a transmission of the encryption code from the telematics unit in response to the emergency event, and ii) transfer the received encryption code to emergency personnel.

2. (Previously presented) The system of claim 1 wherein the transient memory storage is in communication with the key device via a vehicle data network, and wherein the vehicle data network is a local short range wireless network.

3. (Previously presented) The system of claim 1 wherein the key device comprises a key fob, the key fob including:

a controller for receiving the encryption code and storing the encryption code in a persistent memory; and

a transceiver for sending the stored encryption code to the transient memory storage located in the vehicle.

7. (Previously presented) The system of claim 1, further comprising:

a plurality of sensors for detecting damage to the particular vehicle during the emergency event, the plurality of sensors operably connected to the telematics unit, wherein when the emergency event occurs, at least one of the plurality of sensors sends a signal to the telematics unit indicating that the emergency event has occurred.

9. (Previously presented) The system of claim 1 wherein the key device comprises a key including an embedded microchip having a persistent memory storage for storing the encryption code.

10. (Previously presented) The system of claim 3, further comprising:

a biometric sensor located on the key fob and operably connected to the controller, the biometric sensor for sensing biometric data of at least one vehicle user.

11. (Previously presented) A method for providing medical information of a vehicle user, the method comprising:

storing an encryption code in a key device corresponding to a particular vehicle, the encryption code associated with the medical information stored in a database;

transmitting the encryption code from the key device to a vehicle storage unit of the particular vehicle and temporarily storing the transmitted encryption code in the vehicle storage unit prior to an emergency event;

transmitting, from the vehicle storage unit to an in-vehicle telematics unit of the particular vehicle and from the in-vehicle telematics unit to a call center, the temporarily stored encryption code in response to the emergency event involving the particular vehicle;

transmitting the encryption code from the call center to an emergency personnel; and

accessing, via the emergency personnel, the medical information from the database using the encryption code.

13. (Previously presented) The method of claim 20 wherein the transferring of the encryption code from the database to the key device is accomplished using a local short range wireless network or a wired connection.

16. (Previously presented) The method of claim 11 wherein the medical information comprises medical records of the vehicle user.

17. (Previously presented) A system for providing medical information of a vehicle user, comprising:

key device means corresponding to a particular vehicle for receiving and storing an encryption code, the encryption code associated with the medical information of the vehicle user stored in a database;

vehicle storage means of the particular vehicle for i) receiving a transmission of the encryption code from the key device means prior to an emergency event, and ii) temporarily storing the encryption code prior to the emergency event;

an in-vehicle telematics unit of the particular vehicle in communication with the vehicle storage means;

means for transmitting i) from the vehicle storage means to the in-vehicle telematics unit, and ii) from the in-vehicle telematics unit to a call center, the temporarily stored encryption code in response to the emergency event involving the particular vehicle; and

means for accessing, via the emergency personnel, the medical information from the database using the encryption code.

18. (Previously presented) The system of claim 17, further comprising:

means for sensing biometric data of at least one vehicle user, the biometric sensing means located on the key device means; and

means for correlating the sensed biometric data to the medical information of the at least one vehicle user.

19. (Previously presented) The system of claim 1, further comprising a database including the medical information of the vehicle user.

20. (Previously presented) The method of claim 11 wherein prior to storing the encryption code in the key device, the method further comprises:

associating the encryption code with the medical information of the vehicle user;

storing the encryption code in the database; and

transferring the encryption code from the database to the key device.

21. (Previously presented) The method of claim 11 wherein after storing the encryption code in the key device, the method further comprises initiating an ignition cycle of the vehicle.

22. (Previously presented) The method of claim 11 wherein the encryption code is temporarily stored in the vehicle storage unit i) while a vehicle ignition is operating; or ii) for a predetermined amount of time after the vehicle ignition is turned off.

23. (Previously presented) The method of claim 21 wherein upon the initiating of the ignition cycle of the particular vehicle, the method further comprises transmitting the encryption code from the key device to the vehicle storage unit.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.